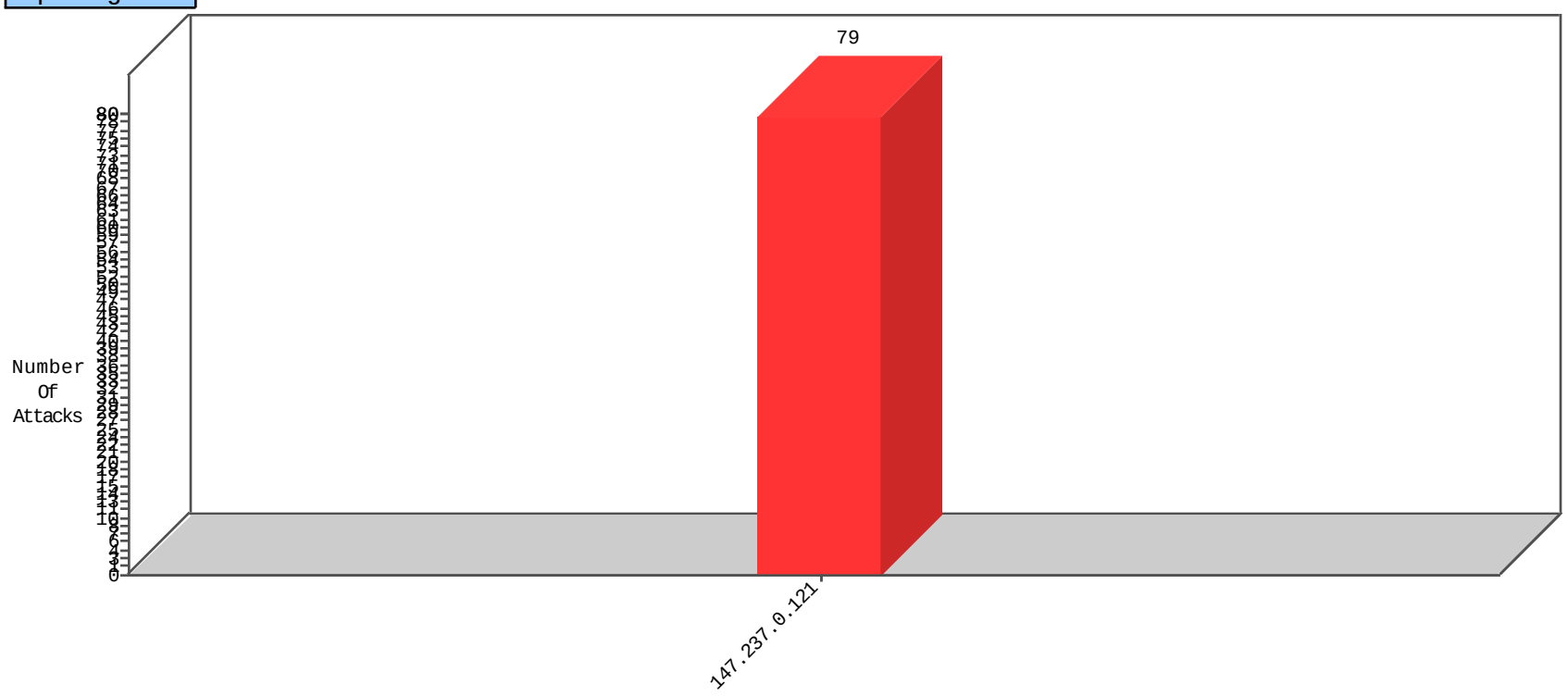
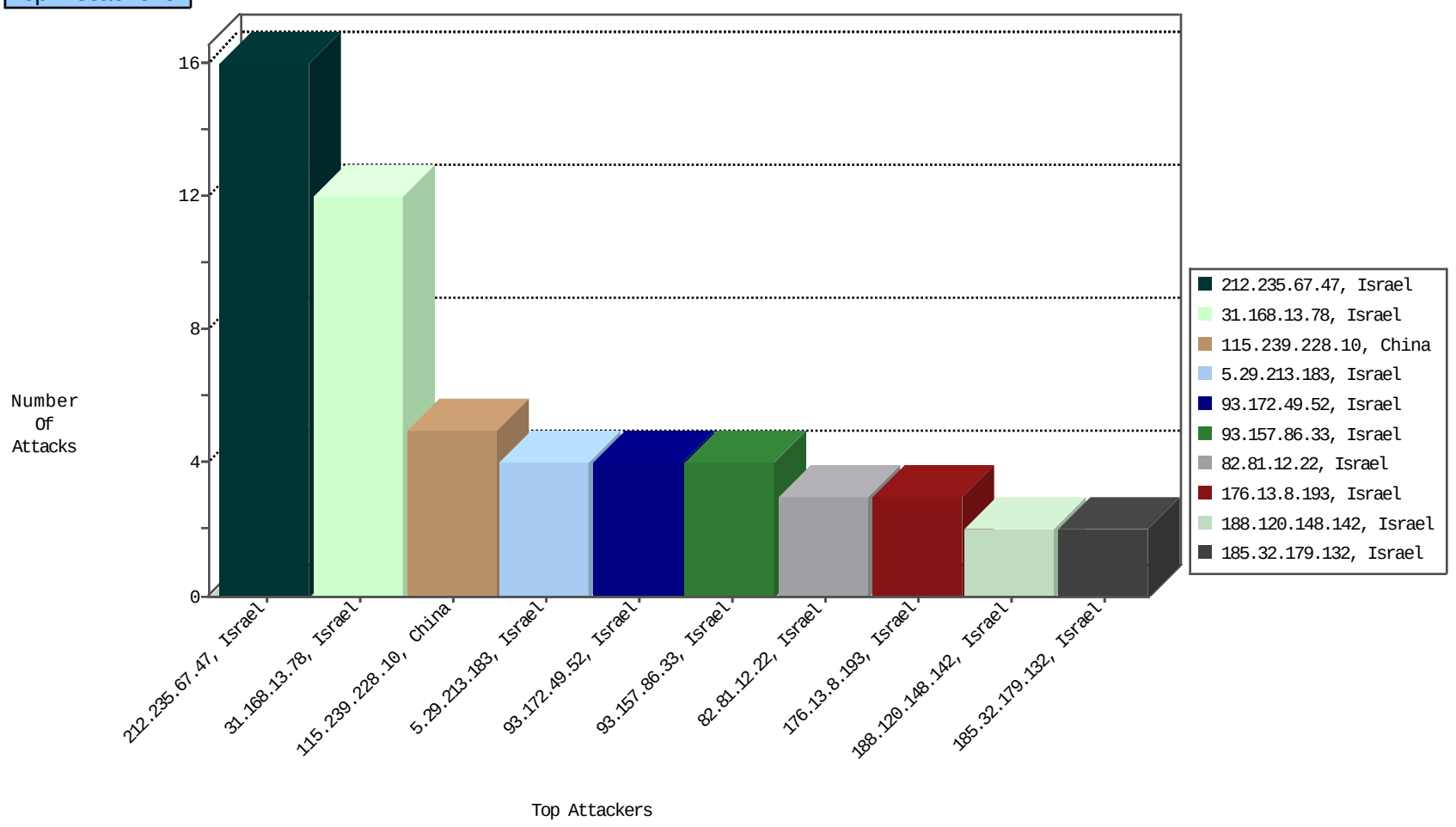
12-23-2015 to 12-24-2015

# Focused IP Under Attack Daily Report

## Top Targets




## Top Attackers



12-23-2015 to 12-24-2015

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | DP_location.Location | Count |
|---|---|---|---|---|---|---|---|
| 82.81.12.22 | Israel | 147.237.0.121 | | Block_Udp_All_Nets | drop | BBL-Israel | 3 |
| 115.239.228.10 | China | 147.237.0.121 | | Frk_Purple_Con_Limit_Http | drop | BBL-Frankfurt | 3 |
| 115.239.228.10 | China | 147.237.0.121 | | Frk_Under_Attack_Con_Http | drop | BBL-Frankfurt | 2 |

12-23-2015 to 12-24-2015

## Top Attackers In IPS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 213.8.204.64 | Israel | 147.237.0.121 | | 13840: TLS: OpenSSL Heartbeat Packet | Block | 2 |

12-23-2015 to 12-24-2015

## Top Attackers In IDS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Count |
|---|---|---|---|---|---|
| 59.45.79.117 | China | 147.237.0.121 | | ET SCAN Potential SSH Scan | 1 |
| 193.105.134.220 | Sweden | 147.237.0.121 | | ET SCAN NMAP -sS window 1024 | 1 |
| 89.231.153.168 | Poland | 147.237.0.121 | | ET SCAN Potential SSH Scan | 1 |
| 208.67.1.131 | United States | 147.237.0.121 | | ET SCAN Potential SSH Scan | 1 |

12-23-2015 to 12-24-2015

## Top Attackers In FW

| Attacker Address | Attacker Geo | Target Address | Site | Name | Signature | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 66.249.93.83 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 2389 |
| 66.249.93.85 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 2346 |
| 66.249.93.89 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 2116 |
| 149.78.47.146 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 598 |
| 194.42.67.50 | United Kingdom | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 336 |
| 66.102.9.87 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 273 |
| 66.249.93.85 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 254 |
| 66.249.93.83 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 249 |
| 66.249.93.89 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 244 |
| 66.102.9.97 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 208 |
| 66.102.9.74 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 177 |
| 2.52.52.147 | Israel | 147.237.0.121 | | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 144 |
| 79.182.112.14 | Israel | 147.237.0.121 | | Bad TCP sequence | SYN retransmit with different window scale | monitor | 107 |
| 149.88.7.255 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 107 |
| 149.78.27.228 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 95 |
| 149.78.134.165 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 91 |
| 13.21.125.9 | United Kingdom | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 76 |
| 157.55.39.54 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 74 |
| 98.216.64.170 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 72 |
| 149.50.71.69 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 50 |
| 149.78.108.102 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 45 |
| 5.29.77.203 | Israel | 147.237.0.121 | | Bad TCP sequence | SYN retransmit with different window scale | monitor | 44 |
| 80.178.203.162 | Israel | 147.237.0.121 | | Bad TCP sequence | SYN retransmit with different window scale | monitor | 43 |
| 217.69.133.252 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 42 |
| 54.88.168.129 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 42 |
| 217.69.133.251 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 40 |
| 193.43.158.229 | Austria | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 39 |
| 149.78.109.19 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 36 |
| 213.16.86.179 | Hungary | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 36 |
| 149.78.223.239 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 36 |
| 82.81.23.71 | Israel | 147.237.0.121 | | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 36 |
| 62.219.129.152 | Israel | 147.237.0.121 | | Bad TCP sequence | Invalid sequence number | monitor | 33 |
| 66.249.74.83 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 26 |
| 66.249.74.81 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 25 |
| 109.64.80.144 | Israel | 147.237.0.121 | | Bad TCP sequence | SYN retransmit with different window scale | monitor | 20 |
| 157.55.39.79 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 20 |
| 46.19.85.129 | Israel | 147.237.0.121 | | Bad TCP sequence | SYN retransmit with different window scale | monitor | 20 |
| 217.69.133.21 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 20 |
| 194.90.233.101 | Israel | 147.237.0.121 | | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 18 |
| 77.127.220.209 | Israel | 147.237.0.121 | | Bad TCP sequence | SYN retransmit with different window scale | monitor | 18 |
| 40.114.210.53 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 18 |
| 217.69.133.249 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 17 |
| 217.69.133.250 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 17 |
| 149.88.81.41 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 16 |
| 94.230.86.143 | Israel | 147.237.0.121 | | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 66.249.93.236 | United States | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 16 |
| 95.131.105.238 | United Kingdom | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 16 |
| 46.19.85.129 | Israel | 147.237.0.121 | | Bad TCP sequence | Invalid sequence number | monitor | 15 |
| 66.249.74.83 | Israel | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 11 |
| 217.69.133.191 | Russian Federation | 147.237.0.121 | | Geo-location enforcement | Geo-location inbound enforcement | drop | 11 |

12-23-2015 to 12-24-2015

## Top Attackers In WAF

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 212.235.67.47 | Israel | 147.237.0.121 | | Unauthorized HTTP Method | Block | 16 |
| 31.168.13.78 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddBoardExamsPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd | Block | 4 |
| 31.168.13.78 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd | Block | 4 |
| 31.168.13.78 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd | Block | 4 |
| 5.29.213.183 | Israel | 147.237.0.121 | | Unauthorized HTTP Method | Block | 4 |
| 93.157.86.33 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest | Block | 4 |
| 176.13.8.193 | Israel | 147.237.0.121 | | Untraceable SSL Sessions: sigalgs DoS Attack | None | 3 |
| 192.198.151.44 | Europe | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/changeunit | Block | 2 |
| 132.64.216.26 | Israel | 147.237.0.121 | | Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify | Block | 2 |
| 188.120.148.142 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting | Block | 2 |
| 93.172.49.52 | Israel | 147.237.0.121 | | Untraceable SSL Sessions: sigalgs DoS Attack | None | 2 |
| 80.246.139.189 | Israel | 147.237.0.121 | | SSL Untraceable Connection - sigalgs DoS Attack | None | 1 |
| 213.57.80.82 | Israel | 147.237.0.121 | | Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/ | Block | 1 |
| 185.32.179.132 | Israel | 147.237.0.121 | | SSL Untraceable Connection - sigalgs DoS Attack | None | 1 |
| 93.172.49.52 | Israel | 147.237.0.121 | | Multiple Untraceable SSL Sessions from 93.172.49.52 (sigalgs DoS Attack) | None | 1 |
| 46.19.86.161 | Israel | 147.237.0.121 | | SSL Untraceable Connection - sigalgs DoS Attack | None | 1 |
| 2.54.1.129 | Israel | 147.237.0.121 | | Multiple Untraceable SSL Sessions from 2.54.1.129 (sigalgs DoS Attack) | None | 1 |
| 83.130.115.227 | Israel | 147.237.0.121 | | Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/ | Block | 1 |
| 93.172.49.52 | Israel | 147.237.0.121 | | SSL Untraceable Connection - sigalgs DoS Attack | None | 1 |
| 79.177.49.236 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 1 |
| 2.54.1.129 | Israel | 147.237.0.121 | | SSL Untraceable Connection - sigalgs DoS Attack | None | 1 |
| 91.231.192.149 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Unknown SSL Session | None | 1 |
| 192.114.91.215 | Israel | 147.237.0.121 | | SSL Untraceable Connection - sigalgs DoS Attack | None | 1 |
| 79.178.107.222 | Israel | 147.237.0.121 | | Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest | Block | 1 |
| 213.8.71.146 | Israel | 147.237.0.121 | | Suspicious Response Code | Block | 1 |
| 185.32.179.132 | Israel | 147.237.0.121 | | Multiple Untraceable SSL Sessions from 185.32.179.132 (sigalgs DoS Attack) | None | 1 |
| 46.19.85.100 | Israel | 147.237.0.121 | | Cookie Tampering on cookie .ASPXAUTH: Expected D05EA63CC62EBF0657F97B64D1A5C85D1DD3588E3886A51759CE7DEB3C0FCB1E5458BF71A906D60D909429E11EC91D9F7853866C00731AA234E1180E77199CF6587B345EB3E9E85238BE130CB94C5ADA39995A2A0FCB64AA574BF8E0AF713A666C95B6FEF040E503852426BFB82C9B55AAD069FC96D08502F6BA240653747D48, Observed 1949C679A46A3FB1C98BF0EC464865176086BC7FF61F780CD72C2C7FD0B2E0478082F3C4CA2C718B381C4D4D1BA717C438440F58DD6D2400619700FE24C16858297FBAD50CEB683B64F7AEB69614F823204ED26C1760FE8114B1E51B962828AF581535 | None | 1 |
| 192.116.190.198 | Israel | 147.237.0.121 | | SSL Untraceable Connection - Open Mode | None | 1 |
| 94.230.82.143 | Israel | 147.237.0.121 | | Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/ | Block | 1 |

12-23-2015 to 12-24-2015